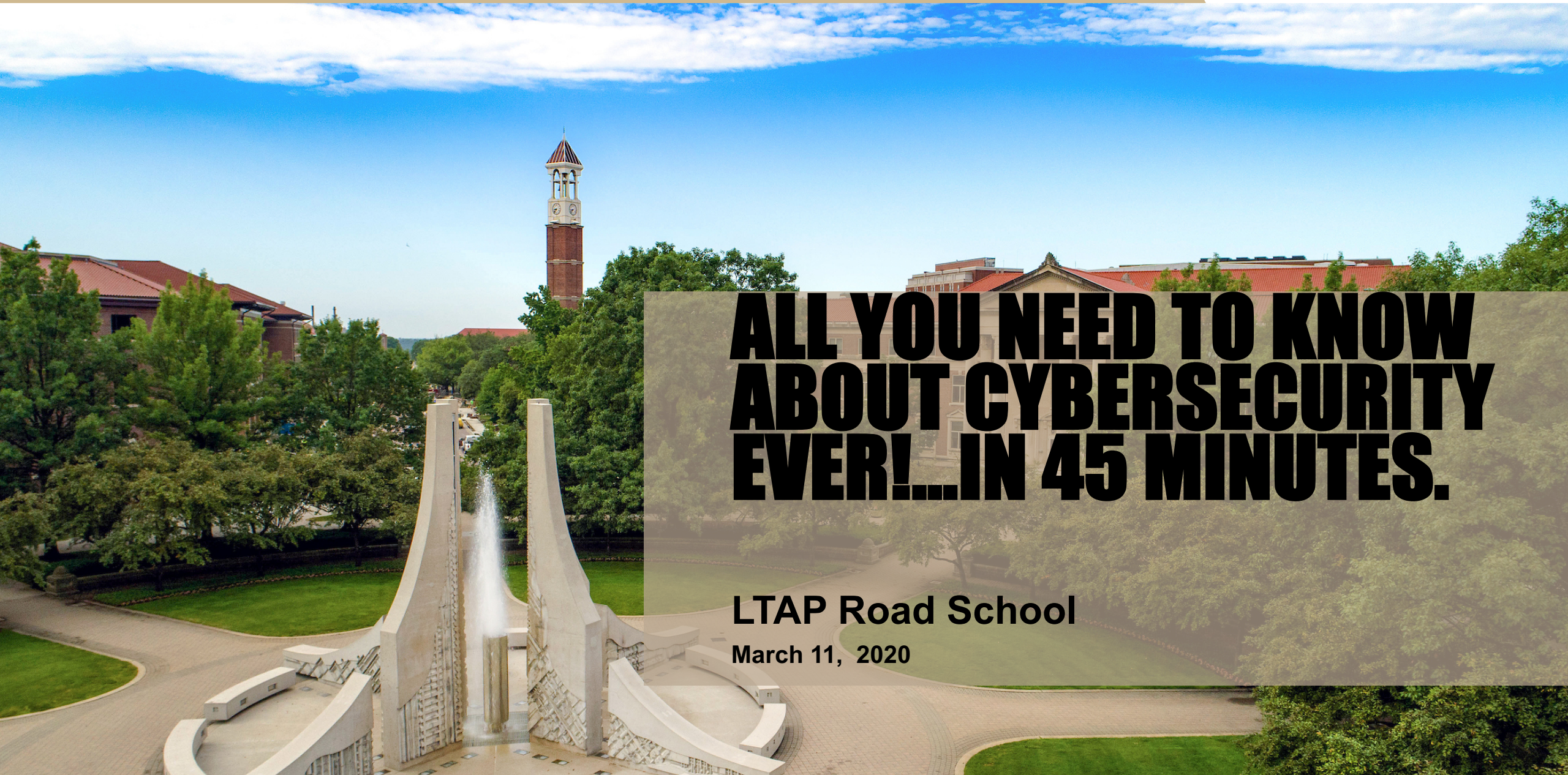


PURDUE UNIVERSITY | cyberTAP

ALL YOU NEED TO KNOW ABOUT CYBERSECURITY EVER!...IN 45 MINUTES.

LTAP Road School

March 11, 2020

PURDUE – CYBER TECHNICAL ASSISTANCE PROGRAM

PURDUE UNIVERSITY | cyberTAP

Mission

cyberTAP exists to help its clients improve their cybersecurity posture through custom-tailored professional services and education

- name: Joe Beckman
- title: Lead Information Security Analyst
- e-mail: beckmanj@purdue.edu
- industry specializations:

  healthcare, local government
- relevant education:

  B.S. Business – IU; MBA – Valpo, Ph.D. in Information Security - Purdue
- relevant experience:

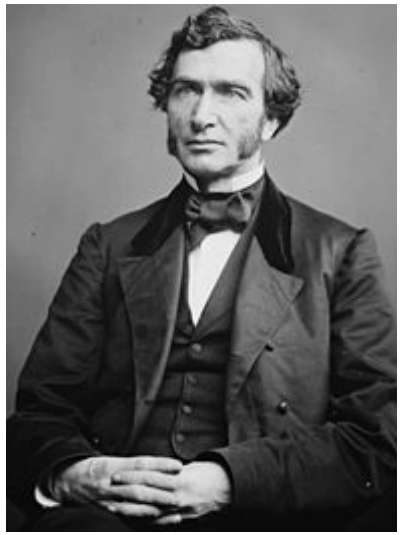
  Deloitte Consulting, CIO/COO/owner of small businesses, USHHS, road medic

AGENDA

- 14:00 – 14:05 -> cyberTAP and You
- 14:05 – 14:15 -> Framing Cybersecurity for Roadways
- 14:15 – 14:45 -> Discussion of Cyber Threats/Controls
- 14:45 – 15:00 -> Q&A

PURDUE'S MISSION AND CYBERTAP

- We're Indiana's "land-grant" University.
  - Morrill Act of 1862
  - Smith-Lever Act of 1914
- We implement our land-grant mission through the "Technical Assistance Program"



"The mission of the Purdue Technical Assistance Program (TAP) is to advance economic prosperity, health, and quality of life in Indiana and beyond."

CYBERTAP'S MAIN FOCUS AREAS

CYBERTAP SERVICES

Purdue curriculum structured for working professionals

Multiple delivery modalities, flexible duration, and customizable content

CYBERTAP SERVICES (2)

Improve your cyber posture with professional cyber consultation services at the highest value.

- *Cyber Risk Assessments*
- *Testing*
- *Vulnerability Scanning*
- *Policy and Practice Consulting*

PURDUE UNIVERSITY | cyberTAP

TAP/CYBERTAP

a service of the Technical Assistance Program &

in the Office of the Executive Vice President for Research and Partnerships

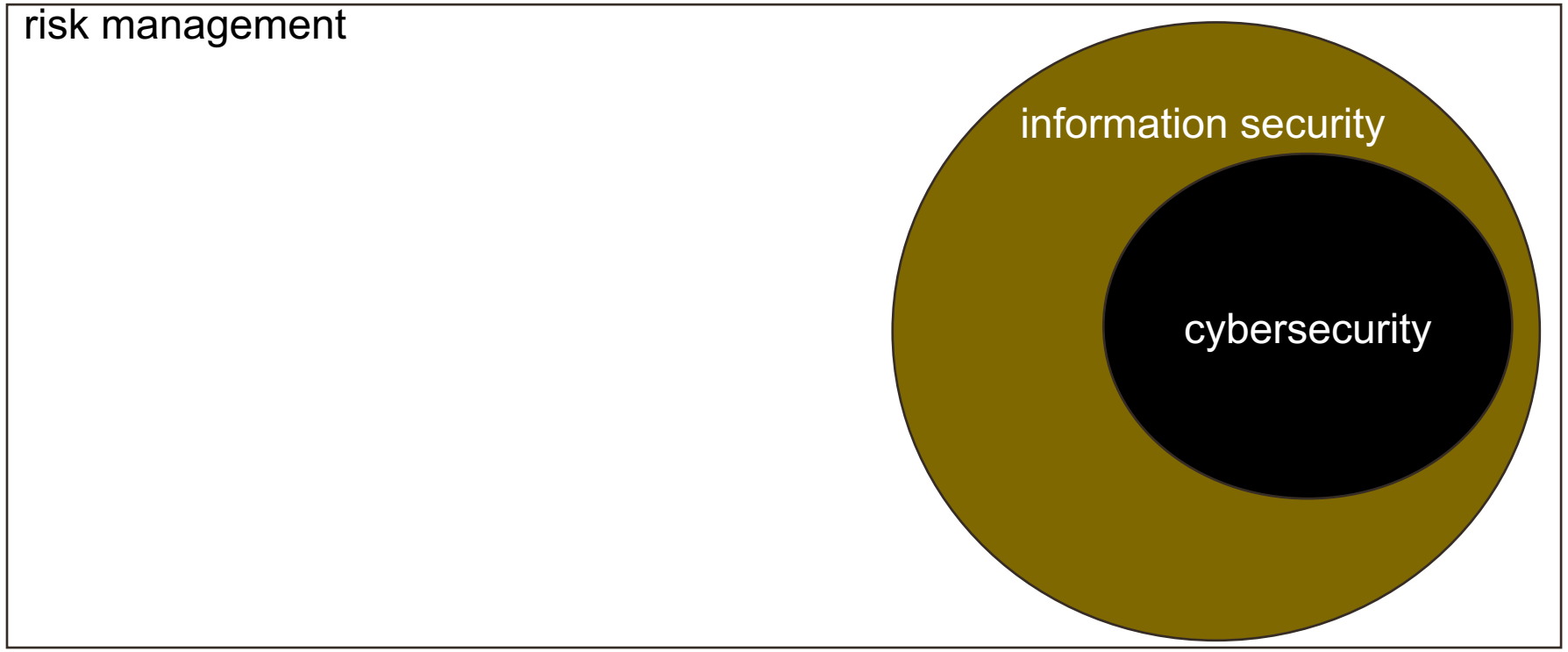
30 Years of TAP Industry Service	**1500+** TAP Clients Served FY19	**~30** Cyber Staff & Students	
~500 FY18/19 - Trained Professionals	**200+** FY19 Cyber Risk Assessments	**$3m+** Sponsored Programs & FFS	

TAP General Stat

cyberTAP Specific Stat

FRAMING “CYBERSECURITY” FOR ROADWAYS

FRAMING CYBERSECURITY



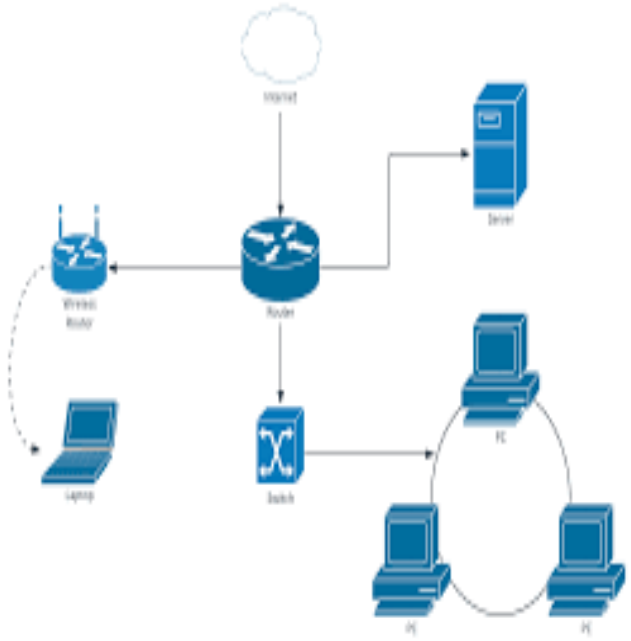
CYBERSECURITY AND ROADWAYS

Graphic Credit: How Technology Can Pave The Future Of Our Roadways. Forbes. 2019

FRAMING OF DEPARTMENTAL CYBERSECURITY RISK

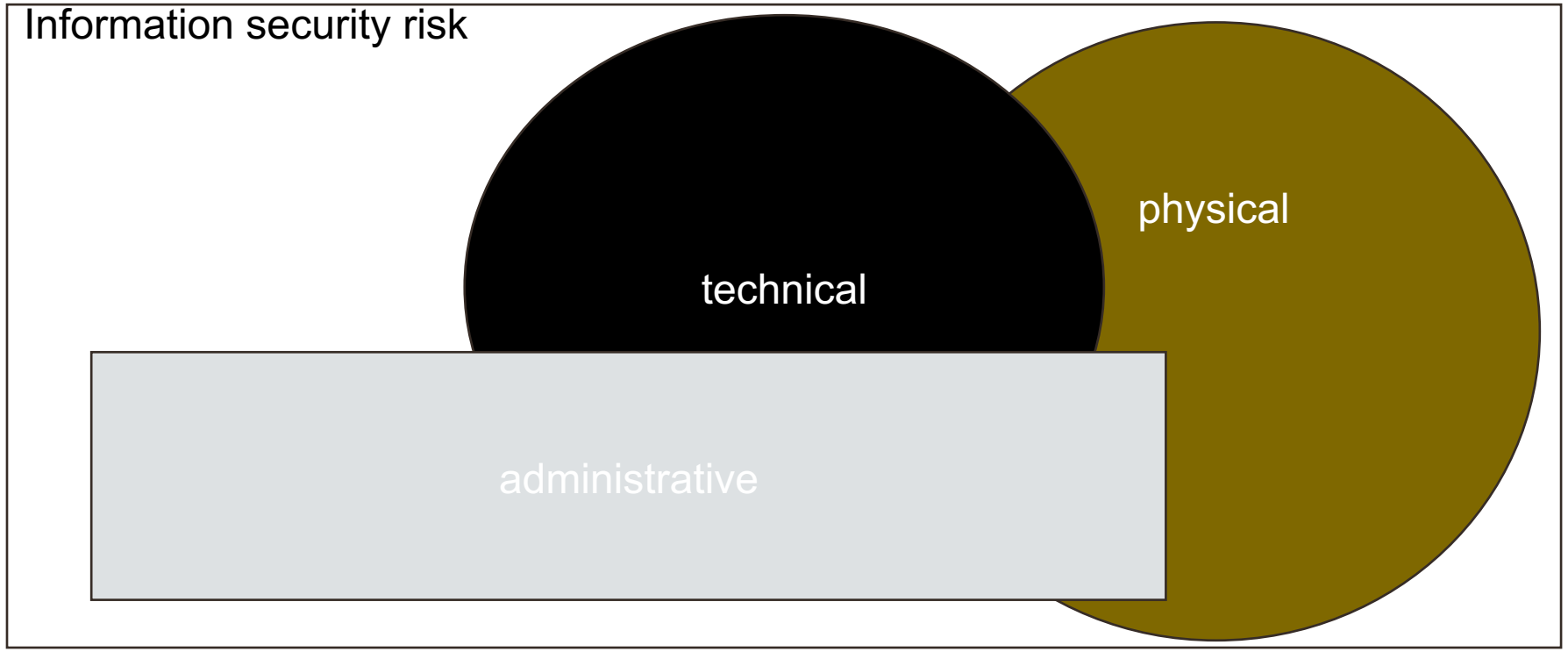
Highway Department

administrative



operations/cyber-physical

FRAMING INFORMATION SECURITY CONTROLS



DEPARTMENTAL CYBERSECURITY RISK - TECHNICAL

Highway Department

administrative

- Microsoft - 57.143%
- Microsoft Windows - 42.857%

operations/cyber-physical

- QEMU - 34.043%
- Microsoft Windows - 29.787%
- Rockwell Automation PLC - 14.894%
- Oracle Linux - 12.766%
- AXIS embedded - 2.128%
- Cisco IOS - 2.128%
- GNU Hurd - 2.128%
- Microsoft - 2.128%

DEPARTMENTAL CYBERSECURITY RISK - ADMINISTRATIVE

Highway Department

administrative

- procedures and training are important, but may be generalizable and rely on existing, common understanding
- not all systems are critical
- monitoring and auditing tends to lag
- devices tend to be homogenous
- **not all systems are critical**

operations/cyber-physical

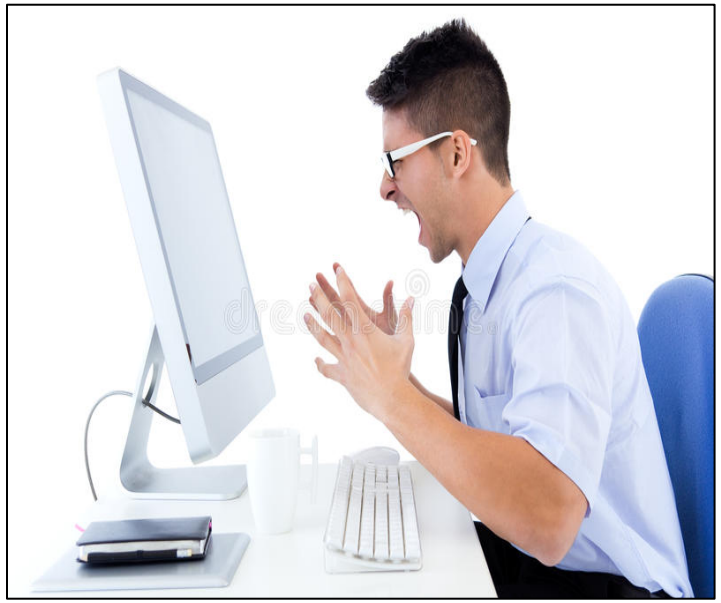
- procedures and training need to be more detailed and well-enforced
- backup and disaster recovery for systems must be well-tested and regularly reviewed
- monitoring and auditing must be regular and thorough.
- devices are diverse
- **in our likelihood X impact model, the impacts of failure are often far more critical**

DEPARTMENTAL CYBERSECURITY RISK - PHYSICAL

Highway Department

administrative

- systems and data are in controlled environments



operations/cyber-physical

- systems, and potentially, data are in uncontrolled environments accessible to unauthorized people and weather

CYBERSECURITY CONTROLS RECOMMENDATIONS

Highway Department

administrative

- use NIST Cybersecurity Framework as a guide
- classify information assets
- perform external and internal assessments
- build new controls/modify to meet the environment
- continuous improvement
- **this network is the normal and regular domain of your IT department**

operations/cyber-physical

- adapt NIST Cybersecurity Framework guidance
- isolate these networks
- create physical barriers to device access by unauthorized beings
- for control devices, have a manual backup
- **Incorporate security into systems design**
- **maintain a close working relationship with IT**

CYBERSECURITY ENVIRONMENT – DEEPER DIVE

TECHNICAL ENVIRONMENT – A USEFUL ANALOGY

operations/cyber-physical

medical devices

- systems and data are in controlled environments, but are critical to patient lives

roadway devices

- critical systems, and potentially, data are in uncontrolled environments accessible to unauthorized people and weather

APPROACH TO SECURITY OF MEDICAL DEVICES

- framework assistance - MDRAP
  - clearinghouse for device-specific technical information
  - container for medical device assessment results
  - aggregator of medical device problems/solutions
- evaluate devices by function
  - is this device transmitting information (telemetry, “kid security”)
  - does this device store information (MRI, CT, infusion pumps)
- secure device directly where possible, isolate functions especially if you can’t control them

APPROACH TO SECURITY OF ROADWAY DEVICES

- Work with IT during pre-purchase to find security concerns
  - what tools does your local gov have to address specific concerns
  - what is the impact of a security failure
  - talk to your peers, share challenges and solutions
- evaluate devices by function
  - is this device transmitting information (bridge sensor, ez-pass)
  - does this device store information (ez-pass transponder, traffic control devices?)
  - How critical is the device/data
- design security in!

APPROACH TO SECURITY OF ROADWAY DEVICES (2)

- Work with IT during pre-purchase to find security concerns
  - what tools does your local gov have to address specific concerns
  - what is the impact of a security failure
  - talk to your peers, share challenges and solutions
- evaluate devices by function
  - is this device transmitting information (bridge sensor, ez-pass)
  - does this device store information (ez-pass transponder, traffic control devices?)
  - How critical is the device/data
- design security in!

EXAMPLES OF CHALLENGES/HACKINGS TO SHARE?

EXAMPLE – DIGITAL ROAD SIGNAGE

- Published hack*:
  - “1 Change the lan of VPN to INTERNET protocol.
  - 2- Scan all the range of the IP on port 23.
  - 3- bruteforce the password.
  - 4- add your message.”
- Defense:
  1. Lock it up. No open panels, change locks with personnel
  2. Disable any unused port.
  3. Use strong passwords, change with personnel.
  4. Monitor road signage regularly.

*https://www.securityweek.com/default-password-exposes-digital-highway-signs-hacker-attacks

EXAMPLE – TRAFFIC SIGNALS (STOP LIGHTS)

- Published hack*:
  1. Accessed unencrypted wireless network
  2. Brute-forced passwords, which were left as default
  3. Updated control database to change lights under different conditions
- Defense:
  1. Encrypt wireless networks
  2. Use strong passwords, change with personnel.
  3. Monitor for database integrity/changes regularly.
  4. Lock cabinets

*Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. (2014). Green lights forever: Analyzing the security of traffic infrastructure. In *8th {USENIX} Workshop on Offensive Technologies ({WOOT} 14)*.

Questions?